Policies, Roles and Responsibilities for Use of the King County Ingress Distributed Security Gateway (a.k.a. Ingress)

August 14, 2007

I. Introduction

This document establishes the Policies and Procedures for agencies to access and use the King County Ingress Distributed Security Gateway (a.k.a Ingress). The Ingress system is required to access a variety of criminal justice applications from outside the King County local area network.

II. Definitions

ACCESS Certification – The designation of a criminal justice practitioner who has received and maintains certified approval by the Washington State Patrol to access state and federal criminal information through the state "ACCESS Switch".

Agency – A government organization, department, or office, with a structure that includes a senior official – appointed chief or director, or elected office – that presides over the organization.

Agency Registrar – An individual from a non-King County agency who administers that agency's users of Ingress. An agency may have more than one registrar.

Application – A computer system that provides data, information, reports, and associated logic for use by individuals.

Application Owner – An agency administrator with responsibility for approving and setting levels of access to an application (or the data within the application) secured within Ingress. This individual can approve, reject and revoke users of the application in question. An application may have more than one owner.

Application User – An individual from an agency that is an authorized user of one or more applications that are secured by Ingress.

Ingress Administrator – A King County OIRM department member that administers Agency Registrars and Application Owners that use Ingress.

Ingress Distributed Security Gateway (a.k.a Ingress) – King County OIRM's security mechanism to give access to law, safety and justice applications that need to be shared with other agencies external to King County.

King County Office of Information Resource Management (OIRM) – The Executive Branch department that manages technology services, computer systems, information security, enterprise projects, telecommunications, and radio services for the county. The department reports to the Chief Information Officer (CIO), who is appointed by the County Executive.

III. Financial Arrangements

Agencies do not have any financial responsibilities under this policy, except that each participant will be responsible for the funding costs it incurs in its own interest, related to the support of this policy. Each Agency shall bear its costs and expenses of using Ingress and any associated applications. Future shared costs, if any, shall be agreed to by all parties.

IV. Liability

Agencies shall indemnify, hold harmless, and defend King County for the use or misuse of information presented in Ingress or any associated applications by their users.

V. King County Service Level

King County will maintain the operation of Ingress following the standards below:

- Ingress will be operational 24 hours a day, 7 days a week, with a standard of 99.9 percent availability excluding scheduled downtime.
- Ingress will be taken offline for maintenance no more than once a month, and no less than once a year. Scheduled downtime will be communicated to all users (Application Owners, Agency Registrars and Application Users) at least 72 hours in advance, in the form of an online alert message within Ingress.
- Unscheduled outages of Ingress may occur from time to time, within the established service levels. When an unscheduled outage occurs, King County, and good faith and to the best of its ability, will attempt to provide an estimated time of recover.
- Applications for which access is hosted within Ingress may be operated by King County OIRM, some other King County agency, or another organization. Each application has its own standards and service levels, which have been established and communicated to Agencies by the Application Owners. It is the responsibility of the application to provide both advanced and ongoing notification to the Application Users when the hosted application is offline.
- King County will attempt to notify Application Users of the unavailable status of any application via Ingress, and may provide advance notification if the County is aware of an outage in advance.

VI. Roles and Responsibilities

A. King County OIRM Responsibilities

King County OIRM shall:

- Establish Ingress Administrators to manage the accounts of Agency Registrars and Application Owners.
- Provide "Help Desk" support for Agency Registrars and Application Owners in the use and functioning of Ingress.
- Take appropriate action within three (3) business days upon notifications regarding changes or terminations for Agency Registrars and Application Owners, or within eight (8) business hours for emergency situations.
- Maintain secure communications, data management, and administrative functionality for the Ingress system and environment.
- Create and distribute auditing reports as defined in the auditing section.

B. Application Owner Responsibilities

Application Owners shall:

- Work with King County OIRM to create and define an application(s) for which access is managed within Ingress.
- Develop policies regarding the agencies with access to certain applications, the users with access to an application, the applicable data restrictions and acceptance criteria for users. (Communication of such policies is the responsibility of the Application Owner, and is outside of Ingress.)
- Respond to requests for access to owned applications within three business days of the request.
- Request from the Agency Registrar and/or requesting Application User's supervisor any additional information needed to respond to a request for access to an application. (This information may differ from application to application.)
- Make the administrative changes needed in both the Ingress application and the application to grant and assign the appropriate access rights to the requesting user.
- If possible, notify OIRM of planned down time for maintenance to be performed on the application by the owner.

C. Agency Responsibilities

Each Agency shall:

- Establish one or more “Agency Registrars” to manage the accounts for each Application User of Ingress secured applications.
- Maintain a sufficient number of Agency Registrars to meet the responsibilities of the registrar function, as determined by the Agency.
- Maintain an up-to-date roster of Agency Registrars and notify King County OIRM of any additions to Agency Registrars or changes in Agency Registrar information.
- Notify King County OIRM to delete any Agency Registrars who are no longer authorized to access Ingress (e.g., due to termination of employment, employment suspension, administrative leave status, etc.), in advance of the cessation of such responsibilities, with an effective date for the removal of the Agency Registrar.

D. Agency Registrar Responsibilities

Agency Registrars shall:

- Identify Application Users authorized to access applications that are secured by Ingress.
- Create user accounts and approve access to Ingress for each Application User.
- Provide complete and accurate records regarding each Application User, including name, job position, department, work contact information, and individual status regarding certain certifications (e.g., Washington State Patrol ACCESS certification).
- Submit requests to Application Owners for access to certain services and applications provided through Ingress.
- Respond to requests for information from an Application Owner regarding users or specific user behavior within three (3) business days.
- Maintain an accurate and up-to-date roster of all Agency Application Users, including the termination of user accounts in Ingress within eight (8) business hours of the termination of the individuals status as an appropriate user (e.g., due to termination of employment, employment suspension, administrative leave status, etc.). Deactivate accounts of Application Users who are on administrative leave in accordance to the rules and policies of the Agency toward work related data while on leave.

E. Application User Responsibilities

Application Users shall:

- Use Ingress, all computer applications, and the data within such applications for official and appropriate law, safety, and justice business purposes only.
- Disseminate data or information only in accordance with applicable laws and policies.
- Provide access to a Ingress secured application only to an authorized person, with appropriate securing of work sites and work stations.
- Follow all application specific policies for use of application data.
- Be approved by local, state and/or federal agencies (all which are applicable) to use and/or view applications/data made available via Ingress.

VII. Auditing

Ingress currently records all login attempts, password changes and application access requests. Future options will include account creations, deletions and resets, and application approvals, rejections and revocations. Ingress does not record individual application activity, though such recording may be performed by the hosted applications.

An Agency Registrar or Application Owner may request audit reports for current auditable items for its agency or applications. Such requests must be made in writing to the Ingress Administrator. Audit reports will be made available to Agency Registrars or Application Owners in a mutually agreed upon electronic format. Agencies and Application Owners may only receive audit information about their agency or applications.

If custom audit reports are requested, King County OIRM may evaluate development costs and request reimbursement for actual expenses associated with report development, depending on the scope of the request.

VIII. Disclosure and Use of Information / Privacy Policy

A. Monitoring and Disclosure of Access and Use of Applications

King County may, in its sole discretion, monitor, record, copy, and inspect any access or activity by any person within applications secured by Ingress. King County may disclose information about any such access or activity to authorized officials within King County or at other agencies, including law enforcement agencies, criminal justice agencies, or courts of competent jurisdiction, and as both allowed and protected by law. By using Ingress, each Agency Registrar and Agency User consents to such monitoring, recording, copying, inspection, and disclosure at the discretion of King County personnel, and as may be required or protected by applicable laws.

B. Use of Personal Information Regarding Registrars or Users

Personal information provided to King County regarding Agency Registrars or Application Users will be used only for purposes of authentication in Ingress for use of authorized applications. Personal information will not be disclosed to any party other than the Ingress Administrator and/or the Application Owner, nor used for any other purpose.

C. Privacy Policy

A copy of King County's privacy policy is available at http://www.metrokc.gov/privacy.aspx. To the extent this policy applies to criminal justice activities, all Agencies, Agency Registrars, Application Owners, Application Users, and Ingress Administrators shall comply with this policy.

IX. Modifications

King County may, at its discretion, modify the policies and procedures for the use of Ingress. Such modifications must be in writing, with the opportunity for the agencies to review and respond to such modifications prior to the modifications taking effect.

X. Duration, Withdrawal and Termination

This policy will remain in effect as long as both the Agency and King County use Ingress, and until such time that King County modifies the agreement. Failure to adhere to these policies by Agency Registrars and Application Users may result in the denial of access to Ingress and associated applications at King County's discretion.

Acknowledgement of Receipt and Certificate of Compliance

I acknowledge receipt of the Policies and Procedures for Use of the King County Ingress Distributed Security Gateway (a.k.a. Ingress). I certify that I am the person responsible for ensuring that my Agency and all Registrar(s) for my Agency comply with these Policies. I further acknowledge that failure by my Agency or any Agency Registrar or Application User to comply with these Policies may result in revocation of access to the Ingress Distributed Security Gateway (a.k.a. Ingress) and/or Ingress-secured applications.

Signature

Title/Position

Name (Print)

Department/Agency

Registrars for my Agency are:

Name	
Title/Position	
Department	
E-Mail Address	
Telephone	( )

Name	
Title/Position	
Department	
E-Mail Address	
Telephone	( )

Name	
Title/Position	
Department	
E-Mail Address	
Telephone	( )

Name	
Title/Position	
Department	
E-Mail Address	
Telephone	( )